FYi

From the Information Policy Analysis Division

Winter 2007
VOLUME 6 ISSUE 2

Meeting the Challenges of Data Practices Training

By Laurie Beyer-Kropuenske
IPAD Director

Providing education and training on data practices and other information policy laws is always challenging.

Trying to explain complex laws often leads to glazed-over eyes and people wishing they could run screaming from the room. As budgets tighten further, it often becomes more difficult to provide live, in-person training to everyone who needs it. In addition, many adult learners expect to receive training that is more flexible and that meets the demands of their schedules. What follows are a number of interesting methods currently in use by a variety of government entities to help educate their employees and others about data practices issues. Some of these may help you jump-start your training efforts.

Obviously, there are other innovative training ideas that IPAD is not aware of. If you are interested in sharing some of your training successes or resources with others, please contact us.

IPAD has developed a new handout, *"Data Practices at a Glance,"* that is useful for training on the broad concepts of the Minnesota Government Data Practices Act. It is especially useful for new managers, commissioners and others who are unaware of state government data practices policies and laws. You can view the handout online at **www.ipad.state.mn.us/docs/dpataglance.pdf**.

IPAD, in collaboration with Minnesota Continuing Legal Education (CLE), is also conducting a series of one-hour web-casts on data practices. The first two web-casts, on January 11 and February 8, covered data practices basics, with a focus on requests for public data, and requests from data subjects. The third session on March 8 will cover a variety of areas that are common to many government entities such as personnel data, trade secret, security information and business data. For more information, contact Minnesota CLE at www.minncle.org. In addition to web-casts, the topic of data practices has been added to the required Managers Core training coordinated by the training unit of the Management Analysis & Development Division of the Department of Administration.

In June 2006, the Minnesota Department of Health (MDH) began sending its employees an informative data practices and security tip of the month to give them practical advice on specific topics. One of the topics recently addressed was protecting private data when you take the data out of the office. In this edition of FYi, we have included two recent tip topics – one on keeping a clean desk and one on password security.

To more efficiently train employees and others on HIPAA responsibilities, the Minnesota Department of Human Services (DHS) worked with Fredrickson Communications, Inc., of Minneapolis, to develop two online training courses, which can be completed in 60-70 minutes.

Data Practices Training
Please see Page 4

Information Policy
Analysis Division

Minnesota
Department of
Administration

Opinion Highlights

*The following are highlights of recent advisory opinions by the Commissioner of Administration. All Opinions are available on the IPAD website, **www.ipad.state.mn.us**.*

06-027: An individual asked whether the Breezy Point City Council complied with Minnesota Statutes, Chapter 13D, the Open Meeting Law, when it held an emergency meeting. The City had received complaints about the services of the existing building inspector and the emergency meeting was held to remove the inspector and hire a new firm to fill that role. The Commissioner wrote that emergency meetings should be used rarely and for circumstances in which public safety is jeopardized. The Commissioner opined that the complaints did not rise to the level of the type of emergency that warranted holding an emergency meeting. Therefore, the Council did not comply with Chapter 13D.

06-028: An individual asked whether the City of Marshall complied with Minnesota Statutes, Chapter 13 in denying a request for the names of applicant finalists. The facts were such that the City considered four candidates as finalists, but at some point in the process two finalists dropped out. The City had previously released the names of the four finalists but then refused to release the names of the two remaining finalists. The Commissioner opined that the names of the two remaining finalists were public data pursuant to section 13.43, subdivision 3.

06-030: The Minnesota Office of Enterprise Technology asked about Minnesota Statutes, section 13.055, which requires government entities to notify individuals after discovering that a breach in security has occurred. The Commissioner wrote that when determining whether a breach of security has occurred, a government entity may consider the fact that the data in question were encrypted. Further, noting there are varying methods and levels of encryption, the Commissioner wrote that an entity should consider the complexity of the encryption and the security of the keys when analyzing whether a breach has occurred.

Opinion Highlights
Please see Page 3

Court Case Update

***Brown* v. *Cannon Falls Township*, 723 N.W.2d 31 (Minn. Ct. App. 2006)**

Landowners in the Cannon Falls Township alleged four separate violations of the Open Meeting Law by members of the Township's board of supervisors. The District Court ordered the board members to pay the required fines, ordered their removal from office, and awarded attorney fees of $13,000 to each landowner.

The Court of Appeals found the district court erred in removing the board members and held the removal of a public official for Open Meeting Law violations requires three or more separate judicial proceedings or adjudications. Filing three or more separate complaints that are tried together is not sufficient for removal. The Court also held that sanctions imposed for specific intent to violate the Open Meeting law were proper because the board members' reliance on their attorney's advice was unreasonable based on the facts of the case. Finally, the Court held that attorney fees are awarded for each action, not per complaint filed, and the award of $13,000 in attorney fees to each landowner was proper. Additional attorney fees cannot be awarded on appeal based on the $13,000 attorney fees cap in the Open Meeting Law.

***EOP-Nicollet Mall, LLC* v. *County of Hennepin*, 723 N.W.2d 270 (Minn. 2006)**

A taxpayer appealed the Tax Court's property tax determination, alleging errors by the Court that required remand for a new trial. One of the alleged errors was that the Tax Court abused its discretion in denying a motion to compel production of private or nonpublic tax data.

The Minnesota Supreme Court held that the Tax Court properly applied the balancing test in Minnesota Statutes, section 13.03, subdivision 6. This balancing test requires a trial court to apply a two-part test to determine whether to compel disclosure of otherwise not public data in response to a motion to compel production of the data. The court must decide whether the data are discoverable and, if so, decide whether the benefit to the party seeking access to the data outweighs any harm to the confidentiality interests involved. The Supreme Court determined that it was not arbitrary or capricious for the Tax Court to conclude the harm of disclosure outweighed the benefit to the taxpayer. The Supreme Court also found it was not erroneous for the Tax Court to order release to the taxpayer of the previously undisclosed data relied on by the opposing side's expert.

Advice from the Swamp Fox*

**Francis Marion, "the Swamp Fox," was a colonial officer from South Carolina in the Revolutionary War renowned for hiding in swamps while carrying out guerilla warfare against the British.*

Dear Swamp Fox:

I am a new Data Practices Compliance Official from Snowy River County. I am preparing a basic data practices training program and would appreciate some guidance on a few aspects of my training.

I frequently receive questions regarding the classifications for data on individuals and data not on individuals. I also receive questions about the different data access rights of the public and individuals about whom public and private data are about. Finally, I receive various questions about the different fees that may be charged for copies of data for public citizens and data subjects.

I know there are differences in the access rights for data subjects and for non-data subjects and I would like to know if there is an effective way to present the answers to these questions in my employee training. Do you have any advice about presenting this information?

Curious Compliance Official

Dear Curious Compliance Official:

The questions you receive present an excellent opportunity for providing some helpful clarification on confusing areas of the Data Practices Act, Minnesota Statutes, Chapter 13.

The classification scheme of the Data Practices Act divides data into two categories: data on individuals or data not on individuals. Data on individuals are separated into three classifications of data: public, private and confidential. Data not on individuals are separated into three different classifications of data: public, nonpublic and protected nonpublic. Data classified as private and nonpublic data are accessible to the data subject (the person whom the data are about), to those employees within a government entity whose work assignments require access, to those entities authorized by law and to those persons with consent from the data subject. Confidential and protected nonpublic data are only available to those entity employees whose work assignments require access to the data and to those entities authorized by law. Confidential and protected nonpublic data are not available to the data subject.

For additional simplification purposes, it is helpful to note that private, nonpublic, confidential and protected nonpublic data can all be called "not public" data. The four "not public" data classifications mean that those data are not available to the public.

You point out that the rights to access data are different depending on whether a member of the public is requesting access to data, or if an individual about whom data are about is requesting access. You are not alone in finding these differences confusing and difficult to present to an audience. I find that the best way to present this type of information is by using comparison charts. There are three charts in the "*From the IPAD Toolbox"* portion of this newsletter that present the information in a helpful way for training purposes. These charts illustrate the data classifications described above, the different timeframes required for inspection and copies of data and whether identification is required, and the different fees that may be charged for copies of government data.

The Swamp Fox

Opinion Highlights

Continued from Page 2

06-032: The City of Mankato asked about the classification of sales receipt data it collects from businesses seeking hardship exemptions from the City's smoking ban ordinance. The Minnesota Department of Revenue provided comments to the Commissioner asserting that because the businesses furnish the data directly to the City, the data are not protected under the tax disclosure laws of Minnesota Statutes, Chapter 270B. The Commissioner agreed, stating that because she was not aware of any law classifying the data in question as anything other than public, the data are public.

07-003: An individual asked whether the Douglas County Sheriff's Office complied with Minnesota Statutes, Chapter 13, when it denied access to certain data from traffic accident reports. The Commissioner opined that the Office's response was not appropriate. Pursuant to Minnesota Statutes, section 169.09, subdivision 13, any data in the accident reports that are of the type listed in section 13.82, subdivisions 3 (request for service data) and 6 (response or incident data), are public and accessible to the public.

Data Practices Training

Please see Page 4

The first course, entitled "Protecting Information Privacy," was developed in coordination with Ramsey County. The second course is "Putting Security into Action." Each year, approximately 6,000 DHS employees and 20,000 county social services staff take the trainings. For more information about the courses, contact David T. Anderson, senior project manager at DHS, 651/431-2150.

In early 2007, Minnesota State Colleges and Universities (MnSCU) will begin pilot-testing online training in data security for all its employees. MnSCU employs about 12,000 people at 32 colleges and universities on 53 campuses.

The training consists of five short "courses," each designed to be completed in about 15 minutes; some are general while others address the handling of specific types of data. The training, developed through collaboration with the University of Minnesota, is copyrighted. For more information contact Ross Janssen, University of Minnesota Privacy and Security Officer, 612/626-5844, **janss006@umn.edu**.

Over the summer, the Minnesota Office of Enterprise Technology began a master planning process. On January 15, 2007, State CIO Gopal Khanna released his agency's report to the Minnesota Legislature. One of the master plan strategies on "information management" identifies data practices education as an important issue. I was among a group of interested state-agency stakeholders who suggested ways to better address issues around information technology and data practices. The strategy recommends required online basic level training in data practices, official records and records management for all state employees.

The plan also calls for addressing the data practices implications of new technologies on the front side, along with systems development and security issues. It also recommends a review of existing information policy laws to see if revisions are needed to take advantage of or effectively deal with technology. The entire report is available at Office of Enterprise Technology's web site; just search "**State IT Master Plan**."

There are many opportunities for training and for sharing information. I hope that I have highlighted a few ideas and resources that you can put to use in your own office.

Data Practices Tips

The following tips on password and workspace security were developed by the Department of Health to assist employees in the proper handling of data.

Password Security:
Data Security / Data Practices Tip of the Month

While we may find them annoying, and even take them for granted, it is important to remember why passwords are important: passwords are often the first (and possibly only) defense against intrusion of our computer systems and the data they contain. Passwords protect private and/or sensitive information – information we don't want anyone and everyone to have access to. As stewards of much private information, MDH has the legal obligation to protect our data from unauthorized access or unintentional exposure. Passwords play a critical role in protecting that information.

Here are some commonsense rules and advice about passwords:

Password Rule 1: Create good (strong) passwords.

Most important, keep your passwords strong by following these rules:

- Use eight or more characters
- Mix upper-case and lower-case letters with numbers and special characters
- Don't use dictionary words, proper nouns or foreign words
- Don't use a correctly spelled word in any language, because "dictionary attack" software can crack these in minutes
- Don't use personal information such as your name (or the name of a relative or pet), birthday or hobby, because these are easy to guess

Choose a password that is difficult to guess or hack, but that you can remember without having to write it down. For example:

- Choose the first letters of words in a title, song or poem: "Book One: Harry Potter and the Sorcerer's Stone" becomes "b1HP&tss"
- String several words together (the resulting password is also known as a "passphrase") and insert numbers and special characters: turn "go to town" into g"o2^*ToWn"
- Insert punctuation or numbers into a regular word: turn "regular" into "rEgu!4lar"

Data Practices Tips
Please see Page 6

From the IPAD Toolbox

The following charts compare aspects of the Data Practices Act (Minnesota Statutes, Chapter 13) regarding data classifications, rights to access data and the fees that may be charged for copies of data.

The first chart summarizes the data classifications within Chapter 13 for data on individuals and data not on individuals.

Data Category	Classification	Meaning of Classification
Data on Individuals/Data not on Individuals	Public/Public	Available to anyone for any reason
Data on Individuals/Data not on Individuals	Private/Nonpublic	Available to: • Data subject • Those whose work requires access • Entities authorized by law • Those authorized by the data subject
Data on Individuals/Data not on Individuals	Confidential/ Protected Nonpublic	Available to: • Those whose work requires access • Entities authorized by law Not available to the data subject

The second chart summarizes the different timeframes in which inspection and copies must be provided for data requests by the data subject and for data requests not by the data subject. The chart also summarizes whether the requestor must provide identification.

	Data Subject Access to Data	Public Access to Data
Inspection of Data	• Must be granted immediately, if possible, or within 10 business days • Entity does not have to disclose the same data for 6 months unless there is a dispute or there are new data	• Must be granted as soon as reasonably possible, and at reasonable times and places within the government entity's control
Copies of Data	• Must be provided immediately, if possible, or within 10 business days	• Must be provided as soon as reasonably possible
Identification	• Required to ensure requestor is the data subject for access to private data, not required for access to public data	• Entity cannot require identification to access public data

The third chart summarizes the different fees that may be charged for copies of data provided to a data subject and copies provided to a requestor who is not the data subject. Additional information about the actual cost that may be charged for providing copies of public data when the requestor is not the data subject is available on IPAD's website at: **www.ipad.state.mn.us/docs/copyfees_1303.doc**.

The Carpenter

	Fees for Data Subject	Fees for Public
Inspection of Data	• No charge/fee	• No charge/fee
Copies of Data	• Maximum charge/fee is actual cost to make, compile, and transmit copies • No charge/fee to search for and retrieve data • No charge/fee to redact private data on others, confidential data, or other "not public" data	• Maximum charge/fee is actual cost to search for and retrieve data, and to make, compile, and transmit copies • Exception: request for 100 paper copies or less – can only charge up to 25¢ per page • No charge/fee for separating public data from "not public" data

- Deliberately misspell a word (don’t use a common misspelling): turn “common” into “koM*7on”

Password Rule 2: Don’t share (No matter what you learned in kindergarten)

When it comes to passwords, it’s not nice to share. Your password is secret and confidential; be sure to keep it that way. Never divulge your password to anyone, whether in person or over the phone – no matter who asks, no matter why they say they need it. If anyone ever asks for your password, report the incident to your supervisor, system administrator or technology help desk, as well as to the MDH Chief Information Security Officer.

Intruders look for passwords posted on your computer, under your keyboard, inside your desk, on your bulletin board and in every other area of your workspace. This is why it’s best not to write down your password at all. But, if you must write it down, treat it like money and keep it in your wallet or another secure location.

Password Rule 3: Don’t let your passwords get stale. Change them periodically

Most computer systems at MDH remind you to change your password periodically; for most systems, this is every 90 days. Consult your division IT support people for specific instructions on changing your passwords. Your password should also be changed immediately if you think for any reason it could have been compromised.

Information Policy
Analysis Division

Questions or comments?

Contact the Information Policy Analysis Division at 201 Administration Building, 50 Sherburne Avenue, St. Paul, MN, 55155; phone 800.657.3721 or 651.296.6733; fax 651.205.4219; email **info.ipad@state.mn.us**.

Staff: Laurie Beyer-Kropuenske, *Director,* Stacie Christensen, Katie Engler, Janet Hey, Linda Miller, Leanne Phinney and Catherine Scott.

This document can be made available in alternative formats, such as large print, Braille or audiotape by calling 651.296.6733.

For TTY communication, contact the Minnesota Relay Service at 800.627.3529 and ask them to place a call to 651.296.6733.

Copyright 2007 by the State of Minnesota, Department of Administration, Information Policy Analysis Division. All rights reserved.

Keep a Clean Desk!

No, we are not talking about vacuuming your office or taking out the trash. Keeping a clean desk means taking steps to protect the security and privacy of the data you may have on your desk and in your office or cubicle, whether it’s in a paper or electronic format. This also means protecting your computer station when you are away from your work area. You should always lock or log out of your workstation when you leave your workspace.

A clean desk ensures that when you’re not at your desk or in your office, sensitive data is properly locked and secured against unauthorized access. It ensures that no inadvertent disclosure of private or otherwise sensitive data occurs.

Clean Desk Rule 1: Lock sensitive paper or computer media away when not in use.

Any information that contains private or otherwise sensitive data should be locked away when your work area is unoccupied or you are gone for the day. Talk to your supervisor or manager for help on this.

Clean Desk Rule 2: Lock your computer or log out when you leave your work area.

Remember to lock your workstation when leaving your work area. A soon-to-be-released Information Security Policy update will mandate securing your computer when you leave your work area. On most Windows workstations, you can press the Ctrl + Alt + Delete keys all at once, then press enter to lock your workstation. On most Windows XP workstations, you can also press the Windows Key + L (L for “Lock”) on your keyboard to do this even quicker. Check with your IT support folks if you need help. Locking your workstation when you step away is a critical step in ensuring your work area is not a source of an unintended disclosure of sensitive data. Virtually all of us work with information that must be protected from unintended disclosure.

Clean Desk Rule 3: Do not post sensitive information in your work area or office.

Keep those items locked up or put away. Some examples of such items include:

- User names and/or passwords
- IP address or detailed network diagrams
- Any private or otherwise sensitive information
- Personnel information
- Anything you would not want disclosed.